



JŪRMALAS VALSTSPILSĒTAS PAŠVALDĪBA

RĪKOJUMS

Jūrmalā

20.05.2022.

Nr. 1.1-14/22/155

Par personas datu aizsardzības noteikumu apstiprināšanu

Pamatojoties uz Eiropas Parlamenta un Padomes regulas Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) 24.panta pirmo daļu, lai nodrošinātu Jūrmalas valstspilsētas pašvaldībā vienotas prasības fizisko personu datu aizsardzībai:

1. Apstiprināt iekšējos noteikumus "Personas datu aizsardzības noteikumi" saskaņā ar šī rīkojuma pielikumu.
2. Jūrmalas valstspilsētas administrācijas Administratīvi juridiskās pārvaldes Kancelejai nosūtīt Jūrmalas valstspilsētas pašvaldības iestāžu un Jūrmalas valstspilsētas administrācijas struktūrvienību vadītājiem apstiprināto noteikumu elektronisko versiju lietvedības sistēmā "Doclogix".
3. Noteikt, ka iekšējo noteikumu "Personas datu aizsardzības noteikumi" 73. un 74. punkts stājās spēkā 2022.gada 1.oktobrī.
4. Ar šo rīkojumu atzīt par spēku zaudējušu 2018.gada 9.maija rīkojumu Nr. 1.1-14/187 "Par iekšējās kārtības "Personas datu apstrādes reģistra veidošanas kārtība" apstiprināšanu".

Izpilddirektors
E.Stobovs

(paraksts*)

***Dokuments parakstīts ar drošu elektronisko parakstu un satur
laika zīmogu.**

Personas datu aizsardzības noteikumi

Izdoti saskaņā ar Eiropas Parlamenta un Padomes regulas Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) 24. panta pirmo daļu un Valsts pārvaldes iekārtas likuma 72. panta pirmās daļas 2.punktu

I. Vispārīgie jautājumi

1. Personas datu aizsardzības noteikumi (turpmāk - noteikumi) nosaka Jūrmalas valstspilsētas pašvaldības (turpmāk - pašvaldība) personas datu aizsardzības tehniskās un organizatoriskās prasības, kas jāievēro apstrādājot personas datus.
2. Noteikumu mērķis ir nodrošināt personu datu apstrādes efektīvu organizēšanu, uzraudzību un aizsardzību, kā arī atbilstību Eiropas Parlamenta un Padomes regulai Nr. 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk - Vispārīgā datu aizsardzības regula) un citu normatīvo aktu prasībām personas datu aizsardzības jomā.
3. Noteikumi attiecas uz visām pašvaldības administrācijas struktūrvienībām, iestādēm, komitejām, komisijām un darba grupām (turpmāk - institūcija), ja pašvaldība ir pārzinis vai apstrādātājs veiktajai personas datu apstrādei un ir saistoši visiem institūciju darbiniekiem, tajā skaitā, bet ne tikai, brīvprātīgā darba veicējiem, praktikantiem un tiem komisiju locekļiem, kuri nav darba tiesiskajās attiecībās ar pašvaldību, kuri, pildot amata pienākumus, ir saistīti ar pašvaldības funkciju nodrošināšanu un veic personas datu apstrādi (turpmāk - darbinieks).
4. Noteikumos lietotie termini ir interpretējami atbilstoši Vispārīgajai datu aizsardzības regulai.

II. Par personas datu aizsardzību atbildīgās personas, to tiesības un pienākumi

5. Par personas datu apstrādi, informācijas resursu un tehnisko resursu drošību ir atbildīgi darbinieki, kuru pienākumi noteikti darba līgumā, amata aprakstā, vai kuri ar rīkojumu ir norīkoti veikt attiecīgos pienākumus.
6. Atbildības sadalījums:
 - 6.1. institūcijas vadītājs atbild par institūcijas veikto personas datu apstrādi saskaņā ar ārējiem normatīvajiem aktiem un pašvaldības iekšējiem normatīvajiem aktiem;
 - 6.2. tiešais vadītājs atbild par tā padotībā esošo darbinieku veikto personas datu apstrādi saskaņā ar ārējiem normatīvajiem aktiem, pašvaldības iekšējiem normatīvajiem aktiem un institūcijas vadītāja rīkojumiem;
 - 6.3. darbinieks atbild par tā veikto personas datu apstrādi saskaņā ar ārējiem normatīvajiem aktiem, pašvaldības iekšējiem normatīvajiem aktiem un tiešā vadītāja rīkojumiem.
7. Pašvaldības personas datu aizsardzības speciālists (turpmāk - datu aizsardzības speciālists) organizē, konsultē un uzrauga personas datu apstrādes atbilstību normatīvo aktu prasībām pašvaldībā saskaņā ar šajos noteikumos noteikto kārtību.
8. Jūrmalas valstspilsētas administrācijas Informācijas un komunikāciju tehnoloģiju pārvalde (turpmāk - tehnisko resursu turētājs) nodrošina loģiskās aizsardzības pasākumus personas datiem, kas glabājas pašvaldības informācijas sistēmās un resursos.
9. Tehnisko resursu turētājam ir šādi pienākumi:
 - 9.1. pēc datu aizsardzības speciālista pieprasījuma sniegt informāciju par informācijas sistēmu lietotājiem un lietotāju pieejas tiesību līmeņiem;
 - 9.2. nodrošināt datu subjekta tiesības uz datu pārnesamību, dzēšanu vai labošanu;
 - 9.3. pēc iespējas nodrošināt integrētas datu aizsardzības principa ievērošanu, ieviešot jaunas vai attīstot esošās informācijas sistēmas;
 - 9.4. sadarboties ar datu aizsardzības speciālistu, lai nodrošinātu personas datu apstrādes drošību.

III. Datu apstrādes organizatoriskā procedūra

10. Personas dati, tostarp īpašo kategoriju dati, kas tiek izmantoti personas datu apstrādē un pēc kuriem ir iespējams identificēt fizisku personu, ir klasificējami kā ierobežotas pieejamības informācija, kurai ir tiesības piekļūt tikai pilnvarotiem darbiniekiem.
11. Personas datu apstrādi, ievērojot normatīvajos aktos noteiktās prasības, veic tikai tie pašvaldības darbinieki, kuru amata pienākumos ietilpst veikt šādas darbības saskaņā ar amata aprakstu, darba līgumu, struktūrvienības nolikumu vai institūcijas vadītāja rīkojumu.
16. Informācijas sistēmās personas datus drīkst apstrādāt tikai tie pašvaldības darbinieki, kuram ir piešķirta attiecīga piekļuve. Darbiniekam ir jāpārziņina sevis veiktās personu datu apstrādes mērķus un tiesiskos pamatus.

17. Personas datu apstrādes laiks ir darba laiks atbilstoši apstiprinātajiem institūcijas darba kārtības noteikumiem vai ārpus institūcijas darba laika, ņemot vērā darbinieka darba specifiku. Personas datu apstrādi veic darba telpās, izņemot gadījumus, kad darbinieks veic drošu attālinātu piekļuvi pašvaldības informācijas sistēmām.
18. Informācijas sistēmu lietotājiem piekļuves tiesības tiek piešķirtas pēc struktūrvienības vadītāja pieprasījuma saskaņā ar pašvaldības iekšējo kārtību par informācijas sistēmu lietošanu.
19. Dokumentus papīra formātā, kas satur īpašo kategoriju datus, darbinieki glabā slēdzamos skapjos, izvērtējot glabāšanas nepieciešamību.
20. Lai nodrošinātu personas datu precizitāti, ņemot vērā mērķus kādiem tos apstrādā, darbinieks:
 - 20.1. neveido nevajadzīgas atsevišķas personas datu kopijas;
 - 20.2. izmanto katru iespēju, lai nodrošinātu personas datu atjaunošanu (piemēram, apkalpojot personu klātienē, lūdz precizēt savu kontaktinformācijai saziņas nolūkā);
 - 20.3. precizē personas datus ja darbinieks konstatē datu neatbilstību.
21. Personas dati tiek apstrādāti un glabāti līdz pašvaldības noteiktā personas datu apstrādes mērķa sasniegšanai, saskaņā ar noteikto lietu nomenklatūru, dokumentu un arhīvu pārvaldības un citu normatīvo aktu prasībām.
22. Dokumentus papīra formātā, kuri satur personas datus, tajā skaitā visus dokumentu sagatavošanas procesā radušos un turpmākam darbam nederīgos pierakstus (arī pašrocīgi veiktos), kuri vairāk nav nepieciešami noteiktā datu apstrādes mērķa sasniegšanai un kuri nav jāsaglabā atbilstoši noteiktajai lietu nomenklatūrai, darbinieks iznīcina, izmantojot papīra smalcinātājus.
23. Īpašu kategoriju personas datus, kurus apstrādā elektroniskā veidā pārsūta citām personām šifrētā veidā vai izmantojot drošus komunikāciju kanālus.
24. Gadījumos, kad Jūrmalas domes (turpmāk - dome) deputātiem pēc domes sēdēm sēžu materiāli papīra formātā vairs nav nepieciešami, tie tiek nodoti iznīcināšanai tam darbiniekam, kurš tos ir izsniedzis.
25. Tehnisko resursu turētājs nodrošina datu nesēju iznīcināšanu, veicot informācijas izdzēšanu un datu nesēju fizisku sabojāšanu, kas neļauj atjaunot to funkcionēšanu. Datu nesēji var tikt nodoti iznīcināšanai ārpalpojuma sniedzējam, ievērojot pakalpojuma līgumā noteiktās prasības un kārtību.
26. Personas datu aizsardzības pārkāpuma konstatēšanas un izmeklēšanas procedūra, kā arī darbinieka rīcība pārkāpuma gadījumā noteikta pašvaldības iekšējos noteikumos par personas datu aizsardzības pārkāpumu atklāšanas, izmeklēšanas un ziņošanas kārtību.

IV. Personas datu aizsardzības organizatoriskā kārtība pašvaldības iestādē

27. Pašvaldības iestādes vadītājs norīko iestādes datu aizsardzības koordinatoru un par koordinatora iecelšanu piecu darba dienu laikā paziņo datu aizsardzības speciālistam. Par koordinatoru ieceļ personu, kura pārzina iestādes darbību, informācijas apmaiņas procesus funkciju nodrošināšanai un kurai ir izpratne par personas datu aizsardzību.
28. Koordinatoram ir pienākums sešu mēnešu laikā kopš norīkošanas, apmeklēt obligāto ievadinstruktažu datu aizsardzības jomā par personas datu apstrādes reģistra lietošanu, ko organizē datu aizsardzības speciālists.
29. Koordinatoram ir šādi pienākumi:
 - 29.1. piedalīties datu subjektam sniedzamās informācijas sagatavošanā atbilstoši datu aizsardzības speciālista norādījumiem;
 - 29.2. sadarbībā ar datu aizsardzības speciālistu piedalīties un uzskaitīt iestādē veiktās personas datu apstrādes darbības, norādot apstrādes darbību, personas datu apstrādes mērķi, personas datu apstrādes tiesisko pamatu; personas datu veidus un saņēmējus, kā arī nodrošināt attiecīgās informācijas aktualizēšanu pašvaldības personas datu aizsardzības reģistrā;
 - 29.3. piedalīties novērtējuma par ietekmi uz datu aizsardzību veikšanā attiecībā uz pašvaldības iestādes veikto personas datu apstrādi;
 - 29.4. piedalīties personas datu aizsardzības pārkāpuma risku izvērtēšanā;
 - 29.5. sadarboties ar datu aizsardzības speciālistu, lai nodrošinātu saskaņotu personas datu aizsardzības prasību ievērošanu iestādē.
30. Koordinatoram ir tiesības:
 - 30.1. saņemt no citiem darbiniekiem pienākumu veikšanai nepieciešamo informāciju;
 - 30.2. saņemt datu aizsardzības speciālista atbalstu pienākumu izpildē.
31. Iestāde var izstrādāt procedūras, kārtības un noteikumus personu datu aizsardzības jomā, saskaņojot tās ar datu aizsardzības speciālistu. Iestādes izstrādātās procedūras, kārtības un noteikumi nedrīkst būt pretrunā ar šiem noteikumiem.

V. Darbinieku tiesības un atbildība

32. Ikviens darbinieks ir atbildīgs par savām veiktajām darbībām ar personas datiem pašvaldības informācijas sistēmās, kas veiktas darbiniekam autorizējoties informācijas sistēmā ar autentifikācijas līdzekļiem.
33. Darbiniekam ir šādi pienākumi:
 - 33.1. personas datus izmantot tikai pašvaldības noteiktajā kārtībā un tikai darba pienākumu izpildei;

- 33.2. pirms personas datu izpaušanas veikt informācijas saņēmēja identificēšanu, pārliecināties par informācijas saņēmēja pilnvarojumu vai tiesībām saņemt personas datus, šābu gadījumā neveicot personas datus saturošas informācijas izplatīšanu, ziņojot par nepamatotiem personas datus saturošas informācijas pieprasījumiem;
 - 33.3. lietot pašvaldības tehnisko aprīkojumu un rīkus ar pienācīgu rūpību un uzmanību, un tikai ar pašvaldības funkciju saistītiem mērķiem, darba līgumā vai amata aprakstā noteikto uzdevumu izpildei;
 - 33.4. neizpaust personas datus un citu informāciju, kuru apstrādā, veicot amata pienākumus, esot darba tiesiskajās attiecībās, kā arī pēc darba tiesisko attiecību izbeigšanas;
 - 33.5. precizēt personas datus, ja ir konstatēta personas datu neprecizitāte, norādot pamatojumu;
 - 33.6. atbilstoši kompetencei nodrošināt, lai telpās, kurās tiek apstrādāti personas dati, trešās personas uzturas tikai darbinieka klātbūtnē;
 - 33.7. beidzot darbu, nodrošināt, lai dokumenti, kuri satur personas datus, tiek novietoti citām personām brīvi nepieejamās vietās;
 - 33.8. izejot no telpas, atstāt datoru tādā stāvoklī, lai darbu ar to varētu atsākt tikai pēc darbinieka autentifikācijas un autorizācijas;
 - 33.9. veicot personas datu apstrādi informācijas sistēmās, izmantot informācijas aizsardzības līdzekļus, kas noteikti informācijas sistēmu lietošanas un drošību reglamentējošajos normatīvajos aktos;
 - 33.10. sadarboties ar tehnisko resursu turētāju un personas datu aizsardzības speciālistu, lai varētu tikt realizētas šajos noteikumos noteiktās tiesības un pienākumi.
34. Darbiniekam ir aizliegts:
- 34.1. informāciju un personas datus glabāt publiski pieejamās vietās un atstāt trešajām personām (arī citiem darbiniekiem) brīvi redzamās vietās, kā arī telefoniski vai citā personu neidentificējošā veidā sniegt informāciju par personas datiem;
 - 34.2. izpaust ziņas par pašvaldības informācijas sistēmu uzbūvi un konfigurāciju, fiziskās un loģiskās aizsardzības līdzekļiem, kā arī atklāt personas datus nepilnvarotām personām vai trešajām personām, izņemot šajos noteikumos noteiktos gadījumos;
 - 34.3. iegūt (tajā skaitā arī aplūkot informācijas sistēmās), izpaust vai nodot personas datus trešajām personām bez tiesiska pamata, kā arī iegūto informāciju izmantot darbībām, kas nav saistītas ar darbiniekam noteiktajiem amata pienākumiem pašvaldības funkciju izpildē;
 - 34.4. izmantot informācijas sistēmas un personas datus personīgām vajadzībām un komerciāliem mērķiem;
 - 34.5. saņemt personas datus patvaļīgi pārveidot, publicēt, piedalīties to nodošanā vai pārdošanā un reproducēt kopumā vai daļēji. Jebkuras darbības ar personas datiem, ieskaitot to vākšanu, reģistrēšanu, ievadišanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un

izpaušanu, bloķēšanu vai dzēšanu, drīkst veikt tikai pašvaldības noteiktā kārtībā amata pienākumu izpildei.

35. Par prettiesiskām darbībām ar personas datiem darbinieku var saukt pie normatīvajos aktos paredzētās atbildības.

VI. Personas datu nodošana trešajām personām

36. Personas datu pieprasījumam jā satur informācija, kas ļauj identificēt datu pieprasītāju un datu subjektu, datu pieprasījuma tiesisko pamatu, kā arī jābūt norādītam pieprasīto datu apjomam un to izmantošanas mērķim. Personas datu nodošana trešajām personām ir iespējama tikai uz rakstiska pieprasījuma pamata.
37. Pirms personas datu nodošanas trešajai personai, darbinieks izvērtē:
37.1. datu nodošanas tiesisko pamatu;
37.2. trešās personas tiesības saņemt pieprasītos personas datus;
37.3. izsniedzamās informācijas apjomu un mērķi.
38. Ja darbinieks konstatē, ka trešajai personai nav tiesības saņemt pieprasītos personas datus vai saņemt tos pieprasītajā apjomā, tiek sagatavots atbilstošs rakstveida atteikums vai daļējs atteikums izsniegt personas datus.
39. Pirms personas datu nodošanas trešajām personām darbinieks nosūtāmo dokumentu saskaņo ar personas datu aizsardzības speciālistu.
40. Sūtot elektroniski trešajām personām informāciju, kas satur personas datus, tajā skaitā īpašo kategoriju personas datus, to pievieno elektroniskā sūtījuma pielikumā, aizsargājot dokumentu (dokumentu arhīvu) ar paroli. Darbinieks sazinās ar informācijas saņēmēju, lai nodotu pielikuma atvēršanas paroli.
41. Nododot personas datus izmantojot informācijas sistēmas, institūcija nodrošina informācijas saglabāšanu par:
41.1. personas datu nodošanas laiku;
41.2. personu, kas nodevusi personas datus;
41.3. personu, kas saņēmusi personas datus.
42. Publicējot vai izsniedzot dokumentus vai to atvasinājumus, atbildīgais darbinieks nodrošina personas datu dzēšanu.
43. Institūcija, kura saņem trešo personu informācijas pieprasījumu un pašvaldības rīcībā nav pieprasīto datu, konsultējoties ar personas datu aizsardzības speciālistu, mēneša laikā rakstiski informē par to datu pieprasītāju.

VII. Novērtējums par ietekmi uz datu aizsardzību un personas datu apstrādes darbību reģistrs

44. Atbildīgais darbinieks, kas ierosina jaunu personas datu apstrādi vai maina esošo personas datu apstrādes procesu uz citu, vienu mēnesi pirms jaunas personas datu apstrādes (piemēram, jauna pakalpojuma, informācijas sistēmas ieviešanas, jaunu saistošo noteikumu projekta

izstrādes, ja tas ietver personas datu apstrādi) uzsākšanas, informē datu aizsardzības speciālistu par plānotās personas datu apstrādes nolūku, personas datu apstrādes tiesisko pamatu, datu subjektu kategoriju, ko plānots apstrādāt, personas datu veidiem, ko plānots apstrādāt, kā arī izmantoto informācijas sistēmu un iesaistītajiem vai plānotajiem apstrādātājiem.

45. Novērtējumu par ietekmi uz datu aizsardzību (turpmāk - novērtējums) pašvaldībā veic, ja plānotā personas datu apstrāde varētu radīt augstu risku datu subjektam normatīvajos aktos un Datu valsts inspekcijas noteiktajos gadījumos.
46. Datu aizsardzības speciālista sagatavotu novērtējuma formu aizpilda koordinators vai darbinieks, kurā pārziņā ir attiecīgais process un personas datu apstrāde. Personas datu aizsardzības speciālists izskata sagatavoto informāciju un, ja nepieciešams, sniedz rekomendācijas risku mazināšanas pasākumu ieviešanai.
47. Datu aizsardzības speciālistam personas datu apstrādes risku izvērtēšanai ir tiesības pieaicināt ārējos ekspertus vai citus attiecīgās jomas speciālistus, kā arī citu institūciju darbiniekus.
48. Personas datu apstrādes darbību reģistru (turpmāk - reģistrs) sadarbībā ar koordinatoriem uztur personas datu aizsardzības speciālists, iekļaujot tajā Vispārīgajā datu aizsardzības regulā noteikto informāciju. Reģistrs tiek uzturēts elektroniskā veidā kā informācijas sistēma, kurai lietotāju piekļuvi piešķir datu aizsardzības speciālists.
49. Koordinatori nodrošina, lai reģistrā attiecībā uz konkrēto institūciju būtu iekļautas visas veiktās personu datu apstrādes, nepieciešamības gadījumā to aktualizējot, par ko koordinators, izmantojot elektronisko pastu, informē personas datu aizsardzības speciālistu.

VIII. Līgumi ar apstrādātājiem

50. Institūcija uzdevumu veikšanai piesaista tikai tādu apstrādātāju (apakšuzņēmēju), kas sniedz pietiekamas garantijas, lai īstenotu normatīvajos aktos noteiktos tehniskos un organizatoriskos pasākumus personas datu aizsardzības un drošības jomā.
51. Institūcija atbild par to, ka līgums ar apstrādātāju ir noslēgts atbilstoši Vispārīgajai datu aizsardzības regulai, tajā ir iekļautas normatīvajos aktos noteiktās minimālās prasības apstrādātājiem personas datu aizsardzības un informācijas tehnoloģiju drošības jomā, kā arī netiek pazemināts pašvaldības izstrādātajos līguma paraugos noteiktais personas datu drošības līmenis.
52. Institūcija līguma projektu, kas paredz personas datu apstrādi, saskaņo ar datu aizsardzības speciālistu.
53. Datu aizsardzības speciālists sniedz rekomendācijas par personas datu prasībām, kas iekļaujami līgumos ar apstrādātājiem.
54. Institūcija, kas noslēgusi līgumu ar apstrādātāju, nodrošina līguma izpildes kontroli personas datu aizsardzības un drošības jomā.

IX. Datu subjekta tiesību nodrošināšana

55. Ja institūcija plāno uzsākt personas datu apstrādi mērķim, par kuru datu subjekts nav informēts, institūcija nodrošina, ka datu subjekts tiek par to informēts pirms apstrādes uzsākšanas, ja personas datus plāno iegūt no datu subjekta, ja vien informācija jau nav viņa rīcībā.
56. Institūcijai ir pienākums sniegt atbildi uz datu subjekta pieprasījumu, ja datu subjekts pieprasa informāciju par sevi vai personu, ko datu subjektam ir tiesības pārstāvēt, ja tas ir adresēts institūcijai vai tas attiecas uz institūcijas pārziņā esošu informāciju, vai funkciju, kuras izpildi nodrošina institūcija. Par visiem datu subjektu pieprasījumiem un sūdzībām, kas skar personas datu apstrādi, institūcijai ir pienākums informēt institūcijas koordinātoru un datu aizsardzības speciālistu.
57. Datu aizsardzības speciālists gatavo atbildi uz datu subjekta pieprasījumu par savu personas datu apstrādi un aizsardzību, ja tas adresēts pašvaldībai kopumā, pamatojoties uz informāciju, ko sniedz institūcijas. Institūcijas atbild par sniegtās informācijas patiesumu un pilnīgumu.
58. Ja datu subjekts vērsas institūcijā ar pieprasījumu nodrošināt viņa, kā datu subjekta tiesības, tad institūcija konsultējoties ar datu aizsardzības speciālistu sniedz atbildi uz datu subjekta pieprasījumu, kā arī veic nepieciešamās darbības, lai nodrošinātu datu subjekta tiesības uz savu personas datu labošanu vai dzēšanu.
59. Sniedzot personas datus datu subjektam, aizliegts izsniegt citu datu subjekta datus, ko pieprasītājam nav tiesības iegūt.
60. Institūcija, sniedzot atbildi datu subjektam, nodrošina, ka informāciju izsniedz tam datu subjektam, kas pieprasījis informāciju un kam ir tiesības iegūt šo informāciju. Ja nepieciešams, institūcijai ir tiesības pieprasīt, lai persona sniedz papildus informāciju, kas ir nepieciešama, lai pārliecinātos par datu subjekta identitāti.
61. Atbildi uz datu subjekta pieprasījumu sniedz mēneša laikā. Šo termiņu var pagarināt vēl uz diviem mēnešiem, ņemot vērā pieprasījumu skaitu pašvaldībā vai institūcijā un datu subjekta pieprasījuma sarežģītību. Institūcija informē datu subjektu par atbildes sniegšanas termiņa pagarinājumu un kavēšanās iemesliem mēneša laikā pēc datu subjekta pieprasījuma saņemšanas.
62. Par liela apjoma informāciju ir uzskatāma informācija, kad datu subjekts pieprasa informāciju, nenorādot laika posmu, par kādu vēlas iegūt informāciju, vai pieprasījums ir adresēts pašvaldībai nevis konkrētai institūcijai un pašvaldībā datu subjekta personas datu apstrāde gada laikā ir veikta vairāk kā trīs institūcijās.
63. Institūcijai ir pienākums informēt datu aizsardzības speciālistu par visiem datu subjekta pieprasījumiem, sniegtajām atbildēm un veiktajām datu apstrādes darbībām, sagatavojot atbildi.

X. Personas datu aizsardzības uzraudzība

64. Datu aizsardzības speciālists neatkarīgi uzrauga personas datu aizsardzību pašvaldībā.

65. Datu aizsardzības speciālists veic pienākumus un funkcijas, kas izriet no Vispārīgās datu aizsardzības regulas prasībām.
66. Datu aizsardzības speciālista tiesības:
 - 66.1. pieprasīt un saņemt no institūcijām savu uzdevumu veikšanai nepieciešamo informāciju un dokumentus, kā arī paskaidrojumus no minēto institūciju darbiniekiem;
 - 66.2. piedalīties pārbaudēs institūcijās personas datu aizsardzības jautājumos;
 - 66.3. sniegt rekomendācijas institūcijām personas datu aizsardzības jomā;
 - 66.4. sniegt konsultāciju datu subjektam par viņa tiesību īstenošanu;
 - 66.5. uzdot institūcijai sniegt novērtējumam nepieciešamo informāciju;
 - 66.6. pieprasīt tehnisko resursu turētājam un pašvaldības izpilddirektoram pieņemt lēmumu par darbinieka auditācijas ierakstu pārbaudi, piekļuves tiesību bloķēšanu vai anulēšanu, ja ir pamatotas aizdomas, ka darbinieks ir veicis nelikumīgu personas datu apstrādi.
67. Datu aizsardzības speciālists pirms pārbaudes uzsākšanas institūcijā par to informē institūcijas vadītāju. Institūcijai ir pienākums nodrošināt institūcijas koordinators klātbūtni datu aizsardzības speciālista pārbaudē institūcijā.
68. Datu aizsardzības speciālists organizē iecelto pašvaldības iestāžu koordinators sanāksmes un apmācības, lai nodrošinātu saskaņotu personas datu aizsardzības prasību ieviešanu un ievērošanu pašvaldībā.
69. Datu aizsardzības speciālists sagatavo un iesniedz pašvaldības izpilddirektoram ziņojumu par iepriekšējā gada personas datu aizsardzības būtiskiem notikumiem pašvaldībā. Datu aizsardzības speciālists nekavējoties ziņo pašvaldības izpilddirektoram par konstatētajiem personas datu aizsardzības pārkāpumiem.
70. Tehnisko resursu turētājam un datu aizsardzības speciālistam ir tiesības:
 - 70.1. saskaņojot ar pašvaldības izpilddirektoru un institūcijas vadītāju, pieprasīt darbiniekiem paskaidrojumus jautājumos, kas saistīti ar personas datu apstrādi;
 - 70.2. sastādīt aktus, atzinumus vai ziņojumus par veikto pārbažu rezultātiem un kopā ar priekšlikumiem par konstatēto nelikumību un trūkumu novēršanu iesniegt pašvaldības izpilddirektoram;
 - 70.3. pārbažu veikšanai, pārskatu un atzinumu sagatavošanai pieaicināt gan ārējos, gan iekšējos auditorus un ekspertus;
 - 70.4. pieprasīt darbiniekiem uzrādīt dokumentus, kas attiecas uz jau veiktu vai plānotu personas datu apstrādi;
 - 70.5. ierosināt un veikt darbības, kas vērstas uz efektīvāku personas datu aizsardzību.
71. Lai nodrošinātu personas datu apstrādes efektīvu uzraudzību un aizsardzību pašvaldībā, konstatējot iespējamu nelikumīgu personas datu apstrādi, tehnisko resursu turētājam un datu aizsardzības speciālistam ir tiesības pieprasīt darbiniekiem veikt kļūdainu vai

nelikumīgi iegūtu datu izdzēšanu vai iznīcināšanu, kā arī lūgt pašvaldības izpilddirektoram noteikt pastāvīgu vai pagaidu aizliegumu personas datu apstrādei un īstenot citus pasākumus, kas nepieciešami personas datu apstrādes uzraudzībai un aizsardzībai.

XI. Darbinieku apmācības

72. Pašvaldība nodrošina savu darbinieku apmācību un informēšanu par datu aizsardzības pasākumiem, veicot sākotnējo apmācību un veicot regulāro apmācību ne retāk kā reizi divos gados. Apmācības tiek organizētas attālinātā veidā vai klātienē, iepazīstinot darbiniekus ar uzlabotajām procedūrām un citos veidos, kas celtu darbinieku zināšanas personas datu aizsardzības jomā.
73. Sākotnējā apmācība tiek nodrošināta darbiniekiem, kuri uzsākuši darba tiesiskās attiecības, un tā veicama ne vēlāk kā viena mēneša laikā no darba tiesisko attiecību uzsākšanas.
74. Sākotnējās apmācības ietvaros darbinieks noklausās video lekciju un izpilda personas datu aizsardzības zināšanu pārbaudes testu, ko sagatavojis datu aizsardzības speciālists.

XII. Noslēguma jautājums

75. Institūcijas vadītājs iepazīstina darbiniekus ar šiem noteikumiem, darbinieks iepazīšanos ar noteikumiem apliecina ar parakstu.